REMARKS

The present Amendment amends claims 1, 13, 25 and 37 and leaves claims 2-8, 14-20 and 26-32 unchanged. Therefore, the present application has pending claims 1-8, 13-20, 25-32 and 37.

Amendments were made to the Abstract so as to clarify the description of the present invention. Entry of these amendments is respectfully requested.

Applicants note that the Examiner did not consider the references cited by an Information Disclosure Statement submitted on February 16, 2001 along with the present application. A copy of said Information Disclosure Statement is attached herewith. An indication that the references cited in therein have been considered is respectfully requested.

Claims 1-8, 13-20, 25-32 and 37 stand rejected under 35 USC §103(a) as being unpatentable over Djakovic (U.S. Patent No. 6,351,539) in view of Coppersmith (U.S. Patent No. 6,189,095). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 1-8, 13-20, 25-32 and 37 are not taught or suggested by Djakovic and Coppersmith whether taken individually or in combination with each other as suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to each of independent claims 1, 3, 25 and 37 from which the other claims depend so as to more clearly describe features of the present invention. Particularly, amendments were made to the claims so as to more clearly

recite that the present invention provides a symmetric key encryption, method, apparatus, medium for storing a program and a program product.

According to the present invention, plain text composed of redundancy data and a message is divided so as to generate a plurality of plain text blocks each having a predetermined length, a random number sequence is generated based on a secret key, and a random number block is generated corresponding to one of the plain text blocks from the random number sequence.

Unique according to the present invention is that a feedback value, obtained a result of operation of one of the plain text blocks and the random number block, is output so that the feedback value can be fed back for use in the operation on another one of the plain text blocks. As per the present invention, an encryption operation is performed using the one plain text block, the random number block and the fed back value so as to produce a cipher text block.

Thus, by use of the present invention after dividing a plain text into a plurality of plain text blocks, an arithmetic operation result of one plain text block is applied to the arithmetic operation of another plain text block. This feature of the present invention is illustrated, for example, in Fig. 10 as F1, F2 and F3.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly the above described features of the present invention are not taught or suggested by Djakovic or Coppersmith whether taken individually or in combination with each other as suggested by the Examiner.

Djakovic teaches a cipher mixer with a random number generator as illustrated, for example, in Fig. 1 thereof. As taught by Djakovic, a block cipher mechanism encrypts a plain text block into a cipher text block. Djakovic further teaches that the encryption operation thereof is limited to the processing of a single plain text block, for example, as illustrated in Figs. 1 and 2. However, at no point is there any teaching or suggestion in Djakovic where the output result of an operation performed on a first plain text block is used for performing an operation on a succeeding plain text block as in the present invention. There is no such teaching of the above described features of the present invention as recited in the claims in Djakovic contrary to the allegations by the Examiner.

In the Office Action the Examiner alleges that Djakovic teaches the feedback mechanism, for example, in col. 2, lines 26-36, wherein it describes that:

> "the second block cipher mechanism takes as input the output of the exclusive-or mechanism and produces a second enciphered output based on the output of the exclusive-or mechanism and on a second key".

The above described teachings of Djakovic are not in anyway related to the generation of a feedback value from an operation on a first plaintext block, wherein the feedback value is fed back for use in an operation on another plain text block as in the present invention as recited in the claims. Djakovic merely teaches a feed forward process wherein, for example, as illustrated in Fig. 2 a first block cipher 18 performs an operation and the output of said operation is fed forward to the exclusive-or 24. The exclusive-or 24 combines a random number and the output of the first block cipher 18 and further feeds forward the output thereof to the second block cipher 20. As per Djakovic the random number is also supplied to a third block

cipher 22 and both the output from the second block cipher 20 and the output from the third block cipher 22 are combined to form an output stream.

At no point is there any teaching or suggestion in Djakovic of a feedback operation as that term is understood by those of ordinary skill in the art. Djakovic simply teaches feed forward processing without returning a result of one processing on first data back so said result can be used in a same processing on another data as in the present invention.

The above described deficiencies of Djakovic are not supplied by any of the other references of record particularly Coppersmith. Therefore, combining the teachings of Djakovic and Coppersmith in the manner suggested by the Examiner in the Office Action still fails to teach or suggest the features of the present invention as now more clearly recited in the claims.

Coppersmith merely discloses a block cipher technique that uses three or more transformation stages for encrypting a plain text block wherein each stage includes a plurality of rounds. The Examiner's attention is directed to, for example, Figs. 3 and 4 and col. 20, lines 7-10 of Coppersmith. In the block cipher mechanism of Coppersmith, an encryption result of one plain text block is not fed back and used to effect encryption of another plain text block. Coppersmith simply divides a plain text block into a plurality of words as illustrated in Fig. 4 and as discussed in col. 15, line 9 through col. 16, line 65 thereof. Fig. 4 of Coppersmith teaches that an operation result of one word is fed forward affecting the operation on other words. Thus, in Coppersmith an encryption operation proceeds with a plurality of words affecting each other in a fed forward manner. However, this operation as taught by

Coppersmith is not a feedback of an output result of a preceding operation on a first set of data for use in the same operation on a second set of data as that term is understood by those of ordinary skill in the art and as recited in the claims.

In the present invention as recited in the claims, the feedback provides that an operation producing an encryption result of a plain text block P_i affects the same operation producing an encryption result of another plain text block P_j. However, the reverse does not occur namely, the encryption result of the block P_j is not used to affect the encryption result of the plain text block P_i.

Thus, Djakovic and Coppersmith fail to teach or suggest outputting a feedback value obtained as a result of operation on the one plain text block and the random number blocks, wherein the feedback value is fed back for use in the operation of another one of the plain text blocks and performing an encryption operation using the one plain text block, the random number block and the feedback value obtained as a result of operation of still another one of the plain text blocks to produce a cipher text block as recited in the claims.

Therefore, as is quite clear from the above, the features of the present invention as now more clearly recited in the claims are not taught or suggested by Djakovic or Coppersmith whether taken individually or in combination with each other as suggested by the Examiner. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 1-8, 13-20, 25-32 and 37 as being unpatentable over Djakovic in view of Coppersmith is respectfully requested.

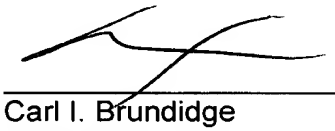
The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 1-8, 13-20, 25-32 and 37.

In view of the foregoing amendments and remarks, applicants submit that claims 1-8, 13-20, 25-32 and 37 are in condition for allowance. Accordingly, early allowance of claims 1-8, 13-20, 25-32 and 37 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.39632X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120